Cariola Díez
Pérez-Cotapos

TECN BITES

NUEVO MARCO DE CIBERSEGURIDAD "NIST CSF V2.0"

El 26 de febrero pasado el Instituto Nacional de Estándares y Tecnología de EEUU (NIST en inglés), publicó la segunda versión de su Marco de Ciberseguridad ("NIST CSF v2.0" o el "Marco"), el cual no había sido actualizado desde el año 2018.

En su versión anterior, el Marco tenía como foco la mejora de la ciberseguridad para infraestructuras críticas, sin embargo, la nueva versión está dirigida a personas responsables de desarrollar y liderar **programas de ciberseguridad en cualquier tipo de organización**, incluyendo pymes.

El NIST CSF v2.0 establece funciones que permiten ir cumpliendo los resultados propuestos. La **gobernanza** es el eje principal del Marco y pone como tarea principal mejorar la comunicación de la gestión de los riesgos, tanto interna como externa.

Así, es primordial que las organizaciones establezcan, comuniquen y monitoreen la estrategia, expectativas y la política de gestión de riesgos de ciberseguridad.

Entendida y establecida dichas funciones, se podrá **identificar** los riesgos actuales a los que está sometida una organización, **proteger** los activos que se identifican en riesgo, **detectar** y analizar los eventuales ataques de ciberseguridad, responder oportunamente ante estos riesgos y **recuperar** los activos u operaciones que fuesen afectados.

En el contexto de la aprobación de la **Ley Marco de Ciberseguridad**, la cual está pendiente de revisión por el Tribunal Constitucional, el NIST CSF v2.0 es una herramienta que permitirá avanzar en la implementación de un sistema de gestión de seguridad de la información continuo, con el fin de determinar aquellos riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional del servicio.

Contacto

Eduardo Vilches
Asociado

José Pablo Lapostol
Asociado